Auditoria-Geral
do Município

GUIA DE ELABORAÇÃO

PLANO DE GERENCIAMENTO DE RISCOS

Vol. 01

Sumário

Introdução

A gestão eficiente dos riscos é essencial para garantir o bom funcionamento das atividades municipais, proporcionando segurança administrativa, eficiência operacional e sustentabilidade institucional. Este guia tem como objetivo oferecer diretrizes claras e estruturadas para identificar, avaliar, tratar e monitorar riscos, garantindo ações proativas e sistemáticas.

Capítulo 1 – Escolha dos Objetos Prioritários (OPs)

Critérios de Seleção

Preliminarmente, devem ser identificados os projetos ou processos prioritários (Objetos Prioritários – OPs) sujeitos à gestão de riscos, observando-se os seguintes critérios:

1. **Materialidade**: Projetos cuja execução envolva montantes financeiros significativos, afetando substancialmente o orçamento e as contas públicas municipais.

2. **Criticidade**: Projetos com histórico frequente de irregularidades detectadas por órgãos internos e externos de controle ou por auditorias internas.

3. **Relevância**: Projetos diretamente alinhados aos objetivos estratégicos definidos pelo Plano Estratégico Institucional vigente.

4. **Inovação**: Projetos com potencial transformador, exigindo elevado grau de inovação tecnológica, metodológica ou administrativa.

Capítulo 2 – Identificação de Riscos

A identificação dos riscos deve envolver todos os agentes relacionados ao processo, desde o planejamento até a supervisão, garantindo a abrangência na identificação dos riscos relevantes.

Classificação dos Riscos

- **Estratégicos**: Decorrentes de decisões gerenciais que influenciam diretamente os objetivos estratégicos.
- **Operacionais**: Resultantes de falhas ou deficiências em processos internos, recursos humanos, infraestrutura física e tecnológica ou sistemas utilizados pelo Município.
- **Conformidade**: Associados a mudanças legislativas ou normativas que possam comprometer as atividades municipais.
- **Integridade**: Relacionados a fraudes, corrupção ou desvios éticos e de conduta que prejudiquem os valores institucionais e a consecução dos objetivos estratégicos e operacionais.

Imagem 01 – Identificação de riscos

IDENTIFICAÇÃO DE RISCOS			
Evento de Risco	**Categoria**	**Possíveis Causas**	**Possíveis Consequências**
Descrever o incidente ou ocorrência que pode afetar negativamente os objetivos	**Estratégico / Operacional / Conformidade / Integridade**	**Elementos que, individualmente ou combinados, tem o potencial para dar origem ao risco**	**Resultados da ocorrência do risco que impactam o objetivo**

Fonte: Ministério do Planejamento e Orçamento (2024)

Avaliação das possíveis causas

CAUSA = FONTES + VULNERABILIDADES	
FONTES DE RISCO	**VULNERABILIDADES**
Pessoas	Em número insuficiente; sem capacitação; perfil inadequado; desmotivadas, alta rotatividade, propensas a desvios éticos e/ou fraudes.
Processos	Mal concebidos (exemplo: fluxo, desenho); sem manuais ou instruções formalizadas (procedimentos, documentos padronizados); sem segregação de funções, sem transparência.
Sistemas	Obsoletos; sem manuais de operação; sem integração com outros sistemas; inexistência de controles de acesso lógico/backups, baixo grau de automação; Infraestrutura física e localização inadequada; instalações ou leiaute inadequados; inexistência de controles de acesso físico.
Tecnologia	Técnica ultrapassada/produto obsoleto; falta de investimento em TI; Tecnologia sem proteção de patentes; processo produtivo sem proteção contraespionagem, controles insuficientes sobre a transferência de dados.
Eventos externos	**Ambientais**: Mudança climática brusca; incêndio, inundação, epidemia; **Econômicos**: oscilações de juros, de câmbio e de preços, contingenciamento, queda de arrecadação, crise de credibilidade, elevação ou redução da carga tributária; **Políticos:** novas leis e regulamentos, restrição de acesso a mercados estrangeiros, ações de responsabilidade de outros gestores; "guerra fiscal" entre estados, conflitos militares, divergências diplomáticas; **Sociais**: alterações nas condições sociais e demográficas ou nos costumes sociais, alterações nas demandas sociais, paralisações das atividades, aumento do desemprego; **Tecnológicos:** novas formas de comércio eletrônico, alterações na disponibilização de dados, reduções ou aumento de custo de infraestrutura, aumento da demanda de serviços com base em tecnologia, ataques cibernéticos;

	Infraestrutura: estado de conservação das vias de acesso; distância de portos e aeroportos; interrupções no abastecimento de água, energia elétrica, serviços de telefonia; aumento nas tarifas de água, energia elétrica, serviços de telefonia. Legais/jurídicos: novas leis e normas reguladoras; novos regulamentos; alterações na jurisprudência de tribunais; ações judiciais.
Governança	Competências e responsabilidades não identificadas ou desrespeitadas; centralização ou descentralização excessiva de responsabilidades; delegações exorbitantes; falta de definição de estratégia de controle para avaliar, direcionar e monitorar a atuação da gestão; deficiência nos fluxos de informação e comunicação; produção e/ou disponibilização de informações, que tenham como finalidade apoiar a tomada de decisão, incompletas, imprecisas ou obscuras; pressão competitiva; falta de rodízio de pessoal; falta de formalização de instruções.
Planejamento	Ausência de planejamento. Planejamento elaborado sem embasamento técnico ou em desacordo com as normas vigentes, objetivos e estratégias inadequados, em desacordo com a realidade.

Fonte: Manual de orientações técnicas da atividade de auditoria interna governamental do Poder Executivo Federal, CGU, 2017.

Caso um evento ou consequência tenham uma mesma causa, estes serão agrupados como um mesmo risco.

Capítulo 3 – Análise e Avaliação de Riscos

Após a identificação, os riscos devem ser avaliados pela combinação de sua probabilidade de ocorrência com o impacto potencial:

Probabilidade x Impacto = Risco Inerente

Escala de Probabilidade		
Magnitude	**Descrição**	**Nota**
Muito Baixa	**Evento improvável de ocorrer.** Excepcionalmente poderá até ocorrer, porém, não há elementos ou informações que indiquem essa possibilidade.	1
Baixa	**Evento raro de ocorrer**. O evento poderá ocorrer de forma inesperada, havendo poucos elementos ou informações que indicam essa possibilidade.	2
Média	**Evento possível de ocorrer.** Há elementos e/ou informações que indicam moderadamente essa possibilidade.	5
Alta	**Evento provável de ocorrer.** É esperado que o evento ocorra, pois os elementos e as informações disponíveis indicam de forma consistente essa possibilidade.	8
Muito Alta	**Evento praticamente certo de ocorrer.** Inequivocamente o evento ocorrerá, pois os elementos e informações disponíveis indicam claramente essa possibilidade.	10

Fonte: Brasil. Tribunal de Contas da União. Roteiro de Auditoria de Gestão de Riscos. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2017. (adaptada)

Escala de Impacto		
Magnitude	**Descrição**	**Nota**
Muito Baixo	Degradação de operações ou atividades de processos, projetos ou programas da organização, porém, causando **impactos mínimos nos objetivos** de prazo, custo, qualidade, escopo, imagem ou relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas (clientes internos/externos, beneficiários).	1
Baixo	Degradação de operações ou atividades de processos, projetos ou programas da organização, causando **impactos pequenos nos objetivos**.	2
Médio	Interrupção de operações ou atividades de processos, projetos ou programas, causando **impactos significativos nos objetivos, porém recuperáveis.**	5
Alto	Interrupção de operações ou atividades de processos, projetos ou programas da organização, causando **impactos de reversão muito difícil nos objetivos.**	8
Muito Alto	Paralisação de operações ou atividades de processos, projetos ou programas da organização, causando **impactos irreversíveis/catastróficos nos objetivos.**	10

Fonte: Brasil. Tribunal de Contas da União. Roteiro de Auditoria de Gestão de Riscos. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2017. (adaptada)

Nível de Risco Inerente (RI)	Resultado do produto
Baixo	Até 9
Médio	Até 39
Alto	Até 79
Extremo	A partir de 80

Fonte: Ministério do Planejamento e Orçamento (2024)

		PROBABILIDADE				
		Muito baixa 1	**Baixa 2**	**Média 5**	**Alta 8**	**Muito Alta 10**
IMPACTO	**10 Muito Alto**	10	20	50	80	100
	8 Alto	8	16	40	64	80
	5 Médio	5	10	25	40	50
	2 Baixo	2	4	10	16	20
	1 Muito baixo	1	2	5	8	10

Fonte: Ministério do Planejamento e Orçamento (2024)

Capítulo 4 – Controle de Riscos

Após apurada a incidência do risco inerente das atividades avaliadas, este deverá ser confrontado com as estruturas vigentes de controle interno, visando determinar claramente o risco residual existente – entendido como aquele que ainda necessita de tratamento específico por parte da Administração.

$$Risco\ Residual\ (RR)\ =\ Risco\ inerente\ x\ Risco\ de\ controle$$

Risco de controle:

Escala de Avaliação Preliminar dos Controles			
Avaliação do Controle*	**Situação do controle existente**	**Nível de Confiança nos controles (NC)**	**Risco de Controle (RC), ou seja, 1 - NC**
Inexistente	Controle não existe, não funciona ou não está implementado.	**Nenhum nível de confiança.**	1,00
Fraco	Controle não institucionalizado; está na esfera de conhecimento pessoal dos operadores do processo; em geral realizado de maneira manual.	**Nível de Confiança de 20%.** Os controles são capazes de mitigar 20% dos eventos.	0,80
Mediano	Controle razoavelmente institucionalizado, mas pode falhar por não contemplar todos os aspectos relevantes do risco ou porque seu desenho ou as ferramentas que o suportam não são adequados.	**Nível de Confiança de 40%.** Os controles são capazes de mitigar 40% dos eventos.	0,60
Satisfatório	Controle institucionalizado e embora passível de aperfeiçoamento, é sustentado por ferramentas adequadas e mitiga o risco razoavelmente.	**Nível de Confiança de 60%.** Os controles são capazes de mitigar 60% dos eventos.	0,40
Forte	Controle institucionalizado e sustentado por ferramentas adequadas, podendo ser considerado em um nível de "melhor prática"; mitiga o risco em todos os aspectos relevantes.	**Nível de Confiança de 80%.** Os controles são capazes de mitigar 80% dos eventos.	0,20
* Não há controle perfeito. Todos têm limitações que impedem que NC seja igual a 1 (um).			

Fonte: Ministério do Planejamento e Orçamento (2024)

Nível de Risco Residual (RR)	Resultado do produto
Baixo	Até 9
Médio	Até 39
Alto	Até 79
Extremo	A partir de 80

Fonte: Ministério do Planejamento e Orçamento (2024)

Capítulo 5 – Tratamento dos Riscos

Os riscos podem ser tratados considerando a natureza, impacto potencial e tolerância da Administração, as principais estratégias de tratamento de riscos são:

Aceitar: Não adotar medidas, dado que o risco residual é baixo ou o custo da mitigação é superior aos benefícios. Justificativas devem ser comunicadas claramente à alta administração.

Mitigar: Implementar medidas que reduzam probabilidade e/ou impacto.

Transferir ou Compartilhar: Reduzir o risco transferindo parcialmente para terceiros, como seguradoras ou prestadores terceirizados.

Evitar: Cessar ou impedir atividades geradoras do risco, eliminando sua possibilidade.

Para seleção da alternativa mais adequada ao tratamento do risco, recomenda-se adotar as seguintes medidas:

1. **Verificação do Custo-benefício:** analisar a relação custo-benefício de cada alternativa de tratamento, considerando-se seu impacto efetivo sobre a probabilidade e o impacto do risco. Devem ser considerados, ainda, os casos em que o tratamento não seja economicamente justificável e os possíveis riscos secundários resultantes das medidas adotadas.

2. **Elaboração do Plano de Tratamento:** desenvolver um plano de ação detalhado e específico para cada risco identificado, contemplando a opção selecionada para tratamento.

3. **Validação dos Controles:** submeter os planos de tratamento ao gestor máximo da unidade para análise e validação quanto à viabilidade econômica e operacional dos controles propostos, priorizando-se aqueles que serão efetivamente executados, considerando custos e esforços necessários à implementação.

4. **Definição do nível de risco aceitável para "apetite a risco":** De acordo com a ISO 31073:2009, apetite ao risco é a "quantidade e tipo de riscos que uma organização está preparada a buscar, reter ou assumir". Com base em um nível de exposição prédefinido, uma organização consegue se adiantar e prever planos de mitigação e correção mais adequados para gerenciar essas ameaças.

Capítulo 6 – Elaboração do Plano de Tratamento

Um **Plano de Tratamento** constitui instrumento estruturado que detalha, de forma clara e objetiva, as ações específicas necessárias para gerenciar adequadamente riscos identificados, atribuindo expressamente sua implementação a um responsável ou equipe designada.

Um plano eficaz permite abordagem preventiva, em oposição à reativa, possibilitando tratamento sistemático e ordenado dos riscos, mitigando, assim, a possibilidade de eventos inesperados e garantindo resposta célere e eficiente diante de eventual materialização.

Sugere-se às unidades administrativas a adoção do seguinte roteiro para elaboração de seus respectivos Planos de Tratamento:

1. **Definição das ações e controles**: indicar, de forma objetiva, as ações específicas a serem adotadas para tratamento do risco identificado. Deve-se esclarecer se haverá mitigação, implementação de salvaguardas ou preparação para cenários futuros, especificando se as medidas envolvem projetos, melhorias de sistemas, criação ou revisão de normas, planos de contingência ou outras ações correlatas. **Ademais, é imprescindível que seja demonstrada a correlação lógica entre a ação proposta e seus efeitos sobre o risco identificado.**

2. **Atribuição de responsabilidades**: estabelecer claramente quem será responsável pela implementação de cada ação, indicando a Secretaria, Diretoria ou Coordenação pertinente, identificando o gestor do objeto da fiscalização ou autoridade designada. Deve-se esclarecer também se haverá envolvimento adicional de outras áreas ou servidores municipais, detalhando como ocorrerá tal participação.

3. **Estabelecimento de prazos e metas**: definir, objetivamente, as tarefas necessárias para a execução das ações propostas, indicando prazos específicos de início e conclusão, com cronograma formalizado, e estabelecendo metas claras e alcançáveis para cada etapa.

4. **Determinação dos recursos necessários**: identificar os recursos financeiros, humanos e materiais indispensáveis para implementação das ações previstas, verificando se já se encontram disponíveis nas unidades responsáveis ou se haverá necessidade de aportes adicionais ou realocação significativa desses recursos, esclarecendo, em qualquer hipótese, o modo como serão providenciados.

Após aprovação formal, o Plano deve ser amplamente divulgado e comunicado a todas as partes interessadas, especialmente à alta administração.

Capítulo 7 – Informação, Comunicação e Monitoramento

A etapa de **Informação e Comunicação** dos riscos organizacionais consiste em atividades executadas ao longo de todo o processo de gestão de riscos, envolvendo o compartilhamento contínuo e estruturado das informações relativas aos riscos identificados e às medidas adotadas para seu tratamento, junto a todos os atores envolvidos.

Essa comunicação deve ser clara, objetiva, pertinente, consistente e tempestiva, assegurando amplo conhecimento sobre os riscos e respectivos tratamentos por parte de todos que atuam direta ou indiretamente no processo.

Além disso, as informações devem estar permanentemente acessíveis às partes interessadas, proporcionando clareza quanto aos respectivos papéis e responsabilidades, garantindo, dessa forma, uma atuação eficiente, eficaz e fundamentada no gerenciamento adequado dos riscos.

As informações devem estar sempre atualizadas e acessíveis no sistema SEI, com monitoramento periódico que responda às seguintes questões essenciais:

- O cronograma estabelecido encontra-se em execução conforme planejado?
- Eventuais atrasos estão sendo devidamente monitorados e os cronogramas ajustados tempestivamente?
- Todos os recursos previstos encontram-se efetivamente disponibilizados?
- De que forma estão sendo registrados e documentados os produtos entregues?
- As informações relativas ao acompanhamento estão atualizadas e devidamente registradas no sistema SEI?
- Houve surgimento de novos riscos desde o último monitoramento realizado?
- A alta administração está sendo regularmente informada acerca do andamento dos trabalhos? De que forma se dá essa comunicação?

Conclusão

Implementar uma gestão estruturada e sistemática dos riscos contribui significativamente para o fortalecimento institucional, melhora a eficiência operacional e protege o Município contra adversidades administrativas e financeiras. A adoção rigorosa deste manual assegurará que o gerenciamento dos riscos se torne parte integrante da cultura organizacional do Município.